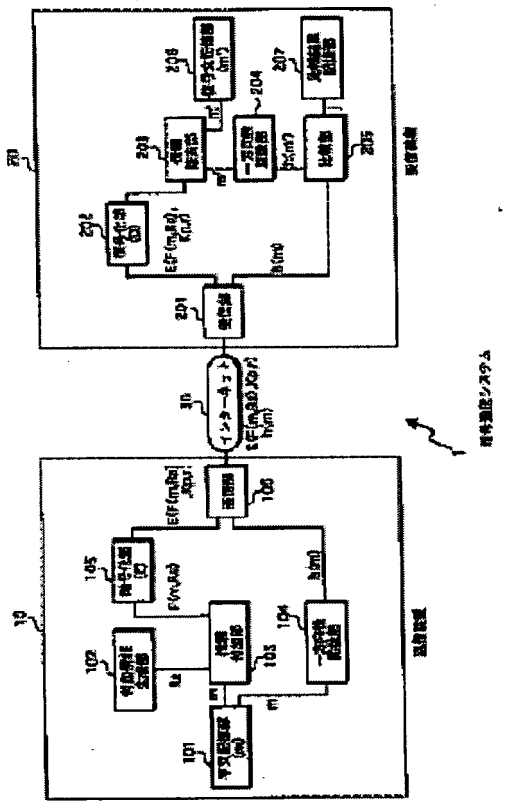
CRYPTOGRAPHIC COMMUNICATION SYSTEM, TRANSMITTER AND RECEIVER

Patent number: JP2002252611
Publication date: 2002-09-06
Inventor: YAMAMICHI MASAHITO; FUDA YUICHI; OMORI MOTOJI; TATEBAYASHI MAKOTO
Applicant: MATSUSHITA ELECTRIC IND CO LTD
Classification:
- international: H04L9/32; G09C1/00
- european:
Application number: JP20010380559 20011213
Priority number(s):

Abstract of **JP2002252611**

PROBLEM TO BE SOLVED: To provide a cryptographic communication system with higher information security.
SOLUTION: A transmitter provides a plaintext with a one-way function to generate a first function value and first additional information, applies a reversible operation to the plaintext and the first additional information to generate joint information, and applies cryptographic algorithm to the joint information to generate a cryptogram. A receiver generates a second additional information similar to the first one, applies decoding algorithm to the cryptogram to generate decoded joint information, applies a reverse operation of the reversible operation to the decoded joint information and the second additional information to generate a decoded sentence, provides the decoded sentence with the one-way function to generate a second function value, compares the first function value with the second one, and determines the decoded sentence to be correct if these two function values agree with each other.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－252611
（P2002－252611A）
(43)公開日　平成14年９月６日(2002.9.6)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/32		Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６７５Ａ	

審査請求　未請求　請求項の数19　ＯＬ　（全 21 頁）

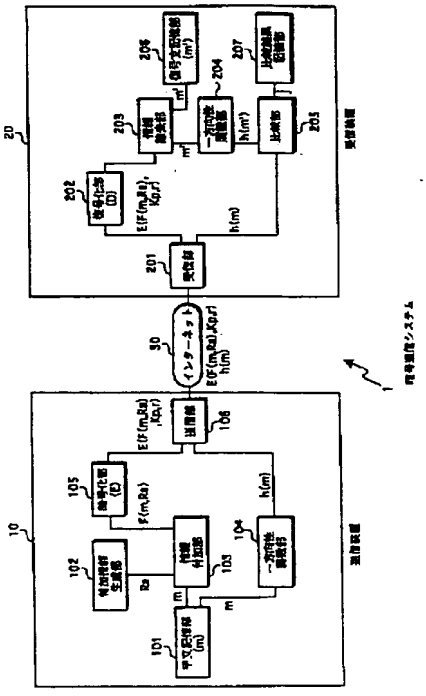
(21)出願番号　特願2001－380559(P2001－380559)
(22)出願日　平成13年12月13日(2001.12.13)
(31)優先権主張番号　特願2000－384835(P2000－384835)
(32)優先日　平成12年12月19日(2000.12.19)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　山道　将人
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　布田　裕一
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　暗号通信システム、送信装置及び受信装置

(57)【要約】
【課題】　さらに安全性の高い暗号通信システムを提供する。
【解決手段】　送信装置は、平文に一方向性関数を施して第１関数値を生成し、第１付加情報を生成し、前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成し、前記結合情報に暗号アルゴリズムを施して暗号文を生成する。受信装置は、第１付加情報と同一の第２付加情報を生成し、前記暗号文に、復号アルゴリズムを施して復号結合情報を生成し、前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成し、復号された復号文に前記一方向性関数を施して第２関数値を生成し、前記第１関数値と前記第２関数値とを比較し、一致する場合に復号文が正当であると判断する。



【特許請求の範囲】

【請求項１】　平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置、及び前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムであって、

送信装置は、

第１付加情報を生成する第１生成手段と、

前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、

前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、

前記暗号文を送信する送信手段とを含み、

受信装置は、

前記暗号文を受信する受信手段と、

前記第１付加情報と同一の第２付加情報を生成する第２生成手段と、

前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、

前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを含むことを特徴とする暗号通信システム。

【請求項２】　前記第１生成手段及び前記第２生成手段は、同期して、それぞれ同一内容の第１付加情報及び第２付加情報を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項３】　前記第１生成手段は、生成した前記第１付加情報を送信し、

前記第２生成手段は、前記第１付加情報を受信し、受信した前記第１付加情報を第２付加情報とすることを特徴とする請求項１に記載の暗号通信システム。

【請求項４】　前記第１生成手段は、生成した前記第１付加情報に暗号アルゴリズムを施して、暗号化付加情報を生成して送信し、

前記第２生成手段は、前記暗号化付加情報を受信し、受信した暗号化付加情報に前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して、付加情報を生成し、生成した付加情報を第２付加情報とすることを特徴とする請求項１に記載の暗号通信システム。

【請求項５】　前記第１生成手段は、乱数を生成し、生成した乱数を前記第１付加情報とすることを特徴とする請求項１に記載の暗号通信システム。

【請求項６】　前記可逆演算手段は、前記平文及び前記第１付加情報に、ビット結合を施して、結合情報を生成し、

前記逆可逆演算手段は、前記復号結合情報から前記第２付加情報を削除して復号文を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項７】　前記可逆演算手段は、前記平文及び前記第１付加情報に、排他的論理和を施して、結合情報を生成し、

前記逆可逆演算手段は、前記復号結合情報及び前記第２付加情報に、排他的論理和を施して、復号文を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項８】　前記可逆演算手段は、前記平文と前記第１付加情報とに加算を施して、結合情報を生成し、

前記逆可逆演算手段は、前記復号結合情報から前記第２付加情報を減じて、復号文を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項９】　前記可逆演算手段は、前記平文及び前記第１付加情報に乗算を施して、結合情報を生成し、

前記逆可逆演算手段は、前記復号結合情報及び前記第２付加情報に逆乗算を施して、復号文を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項１０】　前記可逆演算手段は、前記第１付加情報に基づいて、前記平文のビット表現を置換して、結合情報を生成し、

前記逆可逆演算手段は、前記第２付加情報に基づいて、前記復号結合情報のビット表現を逆置換して、復号文を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項１１】　前記可逆演算手段は、前記第１付加情報に対応する変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記平文を変換して、結合情報を生成し、

前記逆可逆演算手段は、前記第２付加情報に対応し、前記変換テーブルと同一の変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記復号結合情報を逆変換して、復号文を生成することを特徴とする請求項１に記載の暗号通信システム。

【請求項１２】　前記送信装置は、平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成し、その後に再度、前記送信装置は、前記平文と同一の平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成する場合において、

前記第１生成手段は、第１付加情報と異なる第３付加情報を生成し、

前記可逆演算手段は、前記平文及び前記第３付加情報に可逆演算を施して、結合情報を生成し、

前記暗号手段は、前記結合情報に暗号アルゴリズムを施して暗号文を生成し、

前記送信手段は、前記暗号文を送信し、

前記受信手段は、前記暗号文を受信し、

前記第２生成手段は、前記第３付加情報と同一の第４付

加情報を生成し、
前記復号手段は、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成し、
前記逆可逆演算手段は、前記復号結合情報及び第４付加情報に前記可逆演算の逆演算を施して、復号文を生成することを特徴とする請求項１に記載の暗号通信システム。
【請求項１３】　前記送信装置は、前記平文に代えて、生成された前記結合情報に、前記一方向性関数を施して前記第１関数値を生成し、
前記受信装置は、前記復号文に代えて、生成された前記復号結合情報に、前記一方向性関数を施して前記第２関数値を生成し、前記第１関数値と前記第２関数値とが一致するか否かを判断することを特徴とする請求項１に記載の暗号通信システム。
【請求項１４】　前記送信装置は、さらに、前記可逆変換と異なる別の可逆変換を前記平文に施して、別の結合情報を生成し、
前記送信装置は、前記平文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第１関数値を生成し、
前記受信装置は、さらに、生成された前記復号文に、前記別の可逆変換を施して、別の結合情報を生成し、
前記受信装置は、前記復号文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第２関数値を生成し、前記第１関数値と前記第２関数値とが一致するか否かを判断することを特徴とする請求項１に記載の暗号通信システム。
【請求項１５】　平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置、及び前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムで用いられ、送信ステップと受信ステップとを含む暗号通信方法であって、
前記送信ステップは、前記送信装置で用いられ、前記受信ステップは、前記受信装置で用いられ、
送信ステップは、
第１付加情報を生成する第１生成ステップと、
前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆演算ステップと、
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号ステップと、
前記暗号文を送信する送信ステップとを含み、
受信ステップは、
前記暗号文を受信する受信ステップと、

前記第１付加情報と同一の第２付加情報を生成する第２生成ステップと、
前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施し
て復号結合情報を生成する復号ステップと、
前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算ステップとを含むことを特徴とする暗号通信方法。
【請求項１６】　平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置、及び前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムで用いられ、送信ステップと受信ステップとを含む暗号通信プログラムであって、
前記送信ステップは、前記送信装置で用いられ、前記受信ステップは、前記受信装置で用いられ、
送信ステップは、
第１付加情報を生成する第１生成ステップと、
前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆
演算ステップと、
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号ステップと、
前記暗号文を送信する送信ステップとを含み、
受信ステップは、
前記暗号文を受信する受信ステップと、
前記第１付加情報と同一の第２付加情報を生成する第２生成ステップと、
前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号ステップと、
前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算ステップとを含むことを特徴とする暗号通信プログラム。
【請求項１７】　平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置、及び前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムで用いられ、送信ステップと受信ステップとを含む暗号通信プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、
前記送信ステップは、前記送信装置で用いられ、前記受

信ステップは、前記受信装置で用いられ、
送信ステップは、
第１付加情報を生成する第１生成ステップと、
前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆演算ステップと、
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号ステップと、
前記暗号文を送信する送信ステップとを含み、
受信ステップは、
前記暗号文を受信する受信ステップと、
前記第１付加情報と同一の第２付加情報を生成する第２生成ステップと、
前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号ステップと、
前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算ステップとを含むことを特徴とする記録媒体。

【請求項１８】　平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置であって、
第１付加情報を生成する第１生成手段と、
前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、
前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、
前記暗号文を送信する送信手段とを備えることを特徴とする送信装置。

【請求項１９】　平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置から前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置であって、
請求項１８に記載の送信装置から前記暗号文を受信する受信手段と、
前記第１付加情報と同一の第２付加情報を生成する第２生成手段と、
前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、
前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを備えることを特徴とする受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報セキュリティ技術としての暗号技術に関し、特に、復号時の誤り検出

技術に関するものである。

【０００２】

【従来の技術】近年、コンピュータ技術及び通信技術に基づくデータ通信の普及に伴い、特定の通信相手以外に通信内容を漏らすことなくデータ通信を行う暗号通信方式が広く用いられるようになってきており、暗号通信方式を実現するために、暗号方式が用いられる。

【０００３】暗号方式の中には、正規の暗号鍵を用いて平文に暗号アルゴリズムを施して暗号文を生成し、正規の復号鍵を用いて生成した前記暗号文に復号アルゴリズムを施して復号文を生成する場合に、平文と復号文とが異なる可能性がある暗号方式がある。以降、正規の復号鍵を用いて復号しても、復号文が平文と異なることを、「復号誤り」と記述し、復号誤りが生じる可能性がある暗号方式を、「復号誤りが発生し得る暗号方式」と記述する。

【０００４】上記復号誤りが発生し得る暗号方式の一例として、ＮＴＲＵ暗号方式がある。ＮＴＲＵ暗号方式は、簡単に説明すると、暗号鍵を用いて、乱数をパラメータとして用いて、平文を暗号化して暗号文を生成し、復号鍵を用いて、暗号文を復号して復号文を生成する。この方式は、乱数をパラメータとして用いて暗号化するので、平文が同じでも暗号文が異なる可能性がある。

【０００５】なお、ＮＴＲＵ暗号方式については、Jeffrey Hoffstein, Jill Pipher, andJoseph H. Silverman, "NTRU: A ring based public key cryptosystem",Lecture Notes in Computer Science, 1423, pp.267-288,Springer-Verlag, 1998.に詳しく述べられている。ＮＴＲＵ暗号方式を用いる暗号通信方式では、復号文が平文と異なる可能性があるので、意図した情報を確実に伝えることができないという問題がある。

【０００６】（従来例１）上記の問題を解決するために、以下に示すようなＮＴＲＵ暗号方式を用いる暗号通信システムが提案されている。前記暗号通信システムは、暗号装置及び復号装置から構成されている。暗号装置及び復号装置は、通信路で接続されている。暗号装置は、ｎ個の乱数r_1、r_2、・・・、r_nを生成し、予め記憶している暗号鍵Ｋｐを用いて、乱数r_1、r_2、・・・、r_nをパラメータとして用いて、平文ｍを暗号化し、ｎ個の暗号文c_1、c_2、・・・、c_nを生成する。

【０００７】

$c_1 = E(m, Kp, r_1)$

$c_2 = E(m, Kp, r_2)$

・・・

$c_n = E(m, Kp, r_n)$

ここで、Ｃ＝Ｅ（Ｍ、Ｋ、Ｒ）は、暗号鍵Ｋを用いて、乱数Ｒをパラメータとして用いて、平文Ｍを暗号化し、暗号文Ｃを生成することを示す。

【０００８】次に、暗号装置は、生成した暗号文ｃ

c_1、c_2、・・・、c_nを通信路を介して復号装置へ送信する。復号装置は、通信路を介して、ｎ個の暗号文c_1、c_2、・・・、c_nを受信し、予め記憶している復号鍵Ｋｓを用いて、受信した暗号文c_1、c_2、・・・、c_nを復号し、復号文m'_1、m'_2、・・・、m'_nを得る。

【０００９】

$m'_1 = D(c_1, Ks)$

$m'_2 = D(c_2, Ks)$

・・・

$m'_n = D(c_n, Ks)$

次に、復号装置は、上記のようにして得られた復号文m'_1、m'_2、・・・、$m'n$が一つでも異なっていたら復号誤りが発生したとみなす。

【００１０】この暗号通信システムによると、復号誤りの発生が検出できるものの、通信量が増え、非効率的である。また、異なる乱数をパラメータとして用いて、同じ平文を暗号化した複数の暗号文を送信するので、暗号方式の安全性が低下する恐れもある。

$c_1 = E(m, Kp, r_1)$

$c_2 = E(m, Kp, r_2)$

・・・

$c_n = E(m, Kp, r_n)$

のｎ個の関係式から平文ｍや乱数ｒ［１］，ｒ［２］，・・・，ｒ［ｎ］に関する情報が第三者に漏れる恐れがあるからである。このことを利用した暗号攻撃法を、Multiple Transmission Attackと言う。

【００１１】具体的には、復号誤りの発生し得る暗号方式の１つであるＮＴＲＵ暗号方式を用いて、上記復号誤り検出を行うと安全性が低下することが知られている。この攻撃法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem" ,Lecture Notes in Computer Science,1423,pp.267-288,Springer-Verlag, 1998.に詳しく述べられている。

【００１２】以上説明したように、従来例１においては、復号誤りを検出しようとすると、通信量が増大し、しかも安全性が低下する恐れもあるという問題点がある。

（従来例２）また、特開２０００－２１６７７３号公報によると、暗号化された情報の受信側で、復号化した情報が正しいものであるか否かを判定することができる暗号化情報の正当性を判断する方法及び装置を提供することを目的として、以下のような技術が開示されている。

【００１３】情報の発信側では、所定のハッシュ値生成アルゴリズムにより、平文から第１のハッシュ値を算出し、前記第１のハッシュ値と、暗号アルゴリズムを用いて平文を暗号化して得た暗号文とを送信する。情報の受信側では、前記暗号文と、前記第１のハッシュ値とを受信し、前記暗号文を復号して復号文を生成し、前記第１のハッシュ値を算出したハッシュ値生成アルゴリズムと同じアルゴリズムにより前記復号文から第２のハッシュ値を算出し、受信した前記第１のハッシュ値と算出した前記第２のハッシュ値とを比較し、前記第１のハッシュ値と前記第２のハッシュ値とが一致する場合に、前記復号文が正当であると判断する。

【００１４】

【発明が解決しようとする課題】しかしながら、上記の従来技術を適用する場合であっても、第三者による攻撃を完全に避けることは困難であり、従来技術よりもさらに安全性の高い暗号通信システムが要望されている。本発明は、上記の要望に対応するために、さらに安全性の高い暗号通信システム、送信装置、受信装置、暗号通信方法、プログラム及びプログラムを記録している記録媒体を提供することを目的とする。

【００１５】

【課題を解決するための手段】上記目的を達成するために、本発明は、平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置、及び前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムであって、送信装置は、第１付加情報を生成する第１生成手段と、前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、前記暗号文を送信する送信手段とを含み、受信装置は、前記暗号文を受信する受信手段と、前記第１付加情報と同一の第２付加情報を生成する第２生成手段と、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを含むことを特徴とする。

【００１６】ここで、前記第１生成手段及び前記第２生成手段は、同期して、それぞれ同一内容の第１付加情報及び第２付加情報を生成するように構成してもよい。ここで、前記第１生成手段は、生成した前記第１付加情報を送信し、前記第２生成手段は、前記第１付加情報を受信し、受信した前記第１付加情報を第２付加情報とするように構成してもよい。

【００１７】ここで、前記第１生成手段は、生成した前記第１付加情報に暗号アルゴリズムを施して、暗号化付加情報を生成して送信し、前記第２生成手段は、前記暗号化付加情報を受信し、受信した暗号化付加情報に前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して、付加情報を生成し、生成した付加情報を第２付加

情報とするように構成してもよい。

【００１８】ここで、前記第１生成手段は、乱数を生成し、生成した乱数を前記第１付加情報とするように構成してもよい。ここで、前記可逆演算手段は、前記平文及び前記第１付加情報に、ビット結合を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第２付加情報を削除して復号文を生成するように構成してもよい。

【００１９】ここで、前記可逆演算手段は、前記平文及び前記第１付加情報に、排他的論理和を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報及び前記第２付加情報に、排他的論理和を施して、復号文を生成するように構成してもよい。ここで、前記可逆演算手段は、前記平文と前記第１付加情報とに加算を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第２付加情報を減じて、復号文を生成するように構成してもよい。

【００２０】ここで、前記可逆演算手段は、前記平文及び前記第１付加情報に乗算を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報及び前記第２付加情報に逆乗算を施して、復号文を生成するように構成してもよい。ここで、前記可逆演算手段は、前記第１付加情報に基づいて、前記平文のビット表現を置換して、結合情報を生成し、前記逆可逆演算手段は、前記第２付加情報に基づいて、前記復号結合情報のビット表現を逆置換して、復号文を生成するように構成してもよい。

【００２１】ここで、前記可逆演算手段は、前記第１付加情報に対応する変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記平文を変換して、結合情報を生成し、前記逆可逆演算手段は、前記第２付加情報に対応し、前記変換テーブルと同一の変換テーブルをあらかじめ記憶しており、前記変換テーブルに基づいて、前記復号結合情報を逆変換して、復号文を生成するように構成してもよい。

【００２２】ここで、前記送信装置は、平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成し、その後に再度、前記送信装置は、前記平文と同一の平文を暗号化して暗号文を生成して送信し、前記受信装置は、前記暗号文を受信し、受信した暗号文を復号して復号文を生成する場合において、前記第１生成手段は、第１付加情報と異なる第３付加情報を生成し、前記可逆演算手段は、前記平文及び前記第３付加情報に可逆演算を施して、結合情報を生成し、前記暗号手段は、前記結合情報に暗号アルゴリズムを施して暗号文を生成し、前記送信手段は、前記暗号文を送信し、前記受信手段は、前記暗号文を受信し、前記第２生成手段は、前記第３付加情報と同一の第４付加情報を生成し、前記復号手段は、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報及び第４付加情報に前記可逆演算の逆演算を施して、復号文を生成するように構成してもよい。

【００２３】ここで、前記送信装置は、前記平文に代えて、生成された前記結合情報に、前記一方向性関数を施して前記第１関数値を生成し、前記受信装置は、前記復号文に代えて、生成された前記復号結合情報に、前記一方向性関数を施して前記第２関数値を生成し、前記第１関数値と前記第２関数値とが一致するか否かを判断するように構成してもよい。

【００２４】ここで、前記送信装置は、さらに、前記可逆変換と異なる別の可逆変換を前記平文に施して、別の結合情報を生成し、前記送信装置は、前記平文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第１関数値を生成し、前記受信装置は、さらに、生成された前記復号文に、前記別の可逆変換を施して、別の結合情報を生成し、前記受信装置は、前記復号文に代えて、生成された前記別の結合情報に、前記一方向性関数を施して前記第２関数値を生成し、前記第１関数値と前記第２関数値とが一致するか否かを判断するように構成してもよい。

【００２５】

【発明の実施の形態】１．暗号通信システム１

本発明に係る１個の実施の形態としての暗号通信システム１について説明する。

１．１　暗号通信システム１の構成

暗号通信システム１は、復号誤りが発生し得る暗号通信方式における復号誤り検出が可能であるシステムであり、図１に示すように、送信装置１０と受信装置２０とから構成され、送信装置１０と受信装置２０とは、インターネット３０を介して接続されている。

【００２６】暗号通信システム１は、復号誤りが発生し得る暗号方式の一例として、ＮＴＲＵ暗号方式を用いる。ＮＴＲＵ暗号、及びＮＴＲＵ暗号方式の暗号鍵、及び復号鍵の生成方法については、Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, "NTRU: A ring based public key cryptosystem" ,Lecture Notes inComputer Science, 1423, pp.267-288,Springer-Verlag, 1998.に詳しく述べられている。

【００２７】送信装置１０は、予め記憶している平文にＮＴＲＵ暗号方式による暗号アルゴリズムを施して暗号文を生成し、生成した暗号文を受信装置２０へ送信する。受信装置２０は、暗号文を受信し、受信した暗号文にＮＴＲＵ暗号方式による復号アルゴリズムを施して復号文を生成する。

１．２　送信装置１０の構成

送信装置１０は、平文記憶部１０１、付加情報生成部１０２、情報付加部１０３、一方向性関数部１０４、暗号化部１０５及び送信部１０６から構成される。送信装置

１０は、具体的には、具体的には、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボード、マウス、通信部などから構成されるコンピュータシステムである。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。

【００２８】（１）平文記憶部１０１

平文記憶部１０１は、予め平文ｍを記憶している。平文ｍは、固定長の情報から構成される。

（２）付加情報生成部１０２

付加情報生成部１０２は、予め決められたビット数ｒＬｅｎの長さの乱数である付加情報Ｒａを生成し、生成した付加情報Ｒａを情報付加部１０３へ出力する。

【００２９】（３）情報付加部１０３

情報付加部１０３は、平文記憶部１０１から平文ｍを読み出し、付加情報生成部１０２から付加情報Ｒａを受け取る。次に、情報付加部１０３は、読み出した平文ｍと受け取った付加情報Ｒａとを結合して、平文ｍに付加情報Ｒａをビット結合した結果である結合情報Ｆ（ｍ、Ｒａ）＝ｍ｜｜Ｒａを算出する。

【００３０】ここで、演算子「｜｜」は、ビット結合を示す。ビット結合という操作は、２つの値をビット列で表現し、それらを結合したものを１つの値とする操作である。例えば、ｍ＝１０、ｒＬｅｎ＝５、Ｒａ＝７とすると、平文ｍのビット列表現は「１０１０」、長さｒＬｅｎの付加情報Ｒａのビット列表現は「００１１１」となるので、ビット結合した結果は、「１０１００１１１」となり、これは十進数で３２７である。

【００３１】次に、情報付加部１０３は、生成した結合情報Ｆ（ｍ、Ｒａ）を暗号化部１０５へ出力する。

（４）一方向性関数部１０４

一方向性関数部１０４は、予め一方向性関数としてハッシュ関数ｈを有している。

【００３２】ここで、一方向性関数とは、入力された値から関数値を計算することは容易であるが、関数値から関数に入力された元の値を求めることが困難な関数のことである。また、ここで用いるハッシュ関数ｈは、関数の値ｈ（ｍ）から平文ｍの値を得ることが困難であるような十分に安全なもので、かつ衝突困難なものとする。なお、一方向性関数、ハッシュ関数、ハッシュ関数の安全性、及びハッシュ関数の衝突困難性については、「現代暗号」（岡本龍明、山本博資著、シリーズ／情報科学の数学、産業図書、１９９７、５６ページ及び１８９～１９５ページ）に詳しく述べられている。

【００３３】一方向性関数部１０４は、平文記憶部１０１から平文ｍを読み出し、読み出した平文ｍにハッシュ関数ｈによる演算を施して関数値ｈ（ｍ）を生成し、生成した関数値ｈ（ｍ）を送信部１０６へ出力する。

（５）暗号化部１０５

暗号化部１０５は、乱数生成部１０５１、暗号鍵記憶部１０５２及び暗号化関数部１０５３から構成されている。

【００３４】（暗号鍵記憶部１０５２）暗号鍵記憶部１０５２は、予め暗号鍵Ｋｐを記憶している。

（乱数生成部１０５１）乱数生成部１０５１は、一例として、Ｃ言語のライブラリ関数であるｒａｎｄ（　）を用いてる乱数ｒを生成し、生成した乱数ｒを暗号化関数部１０５３へ出力する。

【００３５】（暗号化関数部１０５３）暗号化関数部１０５３は、予めＮＴＲＵ暗号方式の暗号アルゴリズムを有してる。暗号化関数部１０５３は、情報付加部１０３から結合情報Ｆ（ｍ、Ｒａ）を受け取り、乱数生成部１０５１から乱数ｒを受け取り、暗号鍵記憶部１０５２から暗号鍵Ｋｐを読み出す。

【００３６】次に、暗号化関数部１０５３は、受け取った乱数ｒを使用して、読み出した暗号鍵Ｋｐを用いて、受け取った結合情報Ｆ（ｍ、Ｒａ）に前記暗号アルゴリズムを施して、暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ），Ｋｐ，ｒ）を生成し、生成した暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を送信部１０６へ出力する。

（６）送信部１０６

送信部１０６は、暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）と、関数値ｈ（ｍ）とを受け取り、受け取った暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）と、関数値ｈ（ｍ）とをインターネット３０を介して受信装置２０へ送信する。

【００３７】１．３　受信装置２０の構成

受信装置２０は、受信部２０１、復号化部２０２、情報除去部２０３、一方向性関数部２０４、比較部２０５、復号文記憶部２０６及び比較結果記憶部２０７から構成される。受信装置２０は、具体的には、送信装置１０と同様のコンピュータシステムである。

【００３８】（１）受信部２０１

受信部２０１は、送信装置１０からインターネット３０を介して、暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）と関数値ｈ（ｍ）とを受信し、受信した暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を復号化部２０２へ出力し、受信した関数値ｈ（ｍ）を比較部２０５へ出力する。

【００３９】（２）復号化部２０２

復号化部２０２は、復号鍵記憶部２０２１及び復号化関数部２０２２から構成される。

（復号鍵記憶部２０２１）復号鍵記憶部２０２１は、予め復号鍵Ｋｓを記憶している。

【００４０】（復号化関数部２２１０）復号化関数部２２１０は、暗号化関数部１０５３が有する暗号アルゴリズムの逆変換である復号アルゴリズムを予め有している。復号化関数部２２１０は、受信部２０１から暗号化

結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を受け取り、復号鍵記憶部２０２１から復号鍵Ｋｓを読み出す。

【００４１】次に、復号化関数部２２１０は、読み出した復号鍵Ｋｓを用いて、受け取った暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）に前記復号アルゴリズムを施して、復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ）を生成し、生成した復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ）を情報除去部２２５０へ出力する。

【００４２】（３）情報除去部２０３

情報除去部２０３は、予めビット数ｒＬｅｎを記憶している。情報除去部２０３は、復号化部２０２から復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ））、Ｋｓ）を受け取り、受け取った復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ））、Ｋｓ）の末尾からビット数ｒＬｅｎ分のビット列を除去することにより、復号結合情報から付加情報Ｒａを除去し、復号結合情報から付加情報Ｒａが除去された残りの情報を復号文ｍ’として生成し、生成した復号文ｍ’を一方向性関数部２０４へ出力する。また、生成した復号文ｍ’を復号文記憶部２０６へ書き込む。

【００４３】（４）一方向性関数部２０４

一方向性関数部２０４は、一方向性関数部１０４が有しているハッシュ関数ｈと同じハッシュ関数を予め有している。一方向性関数部２０４は、情報除去部２０３から復号文ｍ’を受け取り、受け取った復号文ｍ’にハッシュ関数ｈによる演算を施して関数値ｈ（ｍ’）を生成し、生成した関数値ｈ（ｍ’）を比較部２０５へ出力する。

【００４４】（５）比較部２０５

比較部２０５は、受信部２０１から関数値ｈ（ｍ）を受け取り、一方向性関数部２０４から関数値ｈ（ｍ’）を受け取る。次に、比較部２０５は、関数値ｈ（ｍ）と関数値ｈ（ｍ’）とを比較して、一致するか否かを判断し、一致又は不一致を示す比較結果ｊを生成する。具体的には、比較部２０５は、一致する場合には、比較結果ｊ＝１とし、一致しない場合には、比較結果ｊ＝０とする。次に、生成した比較結果ｊを比較結果記憶部２０７に書き込む。

【００４５】（６）復号文記憶部２０６

復号文記憶部２０６は、復号文を記憶するための領域を備えている。

（７）比較結果記憶部２０７

比較結果記憶部２０７は、比較結果ｊを記憶するための領域を備えでいる。

１．４　送信装置１０の動作

送信装置１０の動作について、図４～図５に示すフローチャートを用いて説明する。

【００４６】付加情報生成部１０２は、付加情報Ｒａを生成し、生成した付加情報Ｒａを情報付加部１０３へ出力する（ステップＳ１０１）。次に、情報付加部１０３は、平文記憶部１０１から平文ｍを読み出し（ステップＳ１０２）、付加情報生成部１０２から付加情報Ｒａを受け取り（ステップＳ１０３）、読み出した平文ｍと受け取った付加情報Ｒａとを結合して、結合情報Ｆ（ｍ、Ｒａ）を生成し、生成した結合情報Ｆ（ｍ、Ｒａ）を暗号化部１０５へ出力する（ステップＳ１０４）。

【００４７】次に、暗号化部１０５は、結合情報Ｆ（ｍ、Ｒａ）を受け取り、受け取った結合情報Ｆ（ｍ、Ｒａ）に暗号アルゴリズムＥを施して暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を生成し（ステップＳ１０５）、生成した暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を送信部１０６へ出力する（ステップＳ１０６）。

【００４８】次に、一方向性関数部１０４は、平文記憶部１０１から平文ｍを読み出し（ステップＳ１０７）、読み出した平文ｍにハッシュ関数ｈによる演算を施して関数値ｈ（ｍ）を生成し（ステップＳ１０８）、生成した関数値ｈ（ｍ）を送信部１０６へ出力する（ステップＳ１０９）。送信部１０６は、暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）と、関数値ｈ（ｍ）とを受け取り、受け取った暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）と、関数値ｈ（ｍ）とをインターネット３０を介して受信装置２０へ送信する（ステップＳ１１０）。

【００４９】１．５　受信装置２０の動作

受信装置２０の動作について、図６に示すフローチャートを用いて説明する。受信部２０１は、送信装置１０からインターネット３０を介して、暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）と関数値ｈ（ｍ）とを受信し（ステップＳ１５１）、受信した暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を復号化部２０２へ出力し、受信した関数値ｈ（ｍ）を比較部２０５へ出力する（ステップＳ１５２）。

【００５０】復号化部２０２は、暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）を受け取り、受け取った暗号化結合情報Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）に復号アルゴリズムＤを施して復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ））を生成し（ステップＳ１５３）、復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ））を情報除去部２０３へ出力する（ステップＳ１５４）。

【００５１】情報除去部２０３は、復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ））を受け取り、受け取った復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ））から付加情報Ｒａを除去して、復号文ｍ’を生成し（ステップＳ１５５）、生成した復号文ｍ’を一方向性関数部２０４へ出力し、生成した復号文ｍ’を復号文記憶部２０６へ書き込む（ステップＳ１５６）。

【００５２】一方向性関数部２０４は、復号文ｍ’を受け取り、受け取った復号文ｍ’にハッシュ関数ｈによる

演算を施して関数値ｈ（ｍ’）を生成し、生成した関数値ｈ（ｍ’）を比較部２０５へ出力する（ステップＳ１５７）。比較部２０５は、関数値ｈ（ｍ）と関数値ｈ（ｍ’）とを受け取り、受け取った関数値ｈ（ｍ）と関数値ｈ（ｍ’）とを比較して、一致するか否かを判断し、一致又は不一致を示す比較結果ｊを生成し、生成した比較結果ｊを比較結果記憶部２０７に書き込む（ステップＳ１５８）。

【００５３】１．６　実施の形態における動作検証と従来例との比較

以下に、本実施の形態における復号誤りの検出について説明する。また、従来技術による方法との比較を行う。復号誤りが発生していない場合において、受信装置２０の比較部２０５が出力する比較結果ｊは常に１である。

【００５４】また、復号誤りが発生している場合に、受信装置２０の比較部２０５が出力する比較結果ｊが１となる確率は、即ち、受信装置２０の一方向性関数部２０４によって生成されたｈ（ｍ’）が、送信装置１０の一方向性関数部１０４によって生成されたｈ（ｍ）と偶然等しくなる確率は、次のようになる。一方向性関数部１０４及び一方向性関数部２０４において、ｋビットのハッシュ値を出力するハッシュ関数を用いる場合、ハッシュ関数により出力されるｋビットのハッシュ値は2^k通り存在するので、前記確率は、2^{-k}となる。

【００５５】従って、実際に復号誤りが発生したとき、受信装置２０により生成される比較結果ｊを調べることによって、$1-2^{-k}$の確率で、復号誤りが発生したことを確認することができる。例えば、一方向性関数部１０４及び一方向性関数部２０４で用いられるハッシュ関数をＳＨＡ－１とするとき、ＳＨＡ－１は１６０ビットの出力を持つので、この確率は$1-2^{-160}$となり、ほぼ復号誤りの発生を検出することができるといえる。

【００５６】また、インターネット３０を介して通信される通信量は、暗号化部１０５が出力する暗号文のビット長と一方向性関数部１０４が出力するハッシュ値のビット長を合わせた量である。一般にハッシュ関数の出力ビット長は入力データの出力ビット長よりも小さいので、この例での通信量は、暗号文の出力ビット長の２倍を越えることはない。

【００５７】例えば、ハッシュ関数にＳＨＡ－１を使う場合、ＮＴＲＵ暗号方式を含む暗号方式では暗号文長が１６０ビット以上のものが使われることが多いので、このことは成り立つ。従来例１のデータ暗号化システムの通信量は、暗号文の出力ビット長の複数倍であったので、従来例１のデータ暗号化システムに比べて、この本実施の形態では通信量が少なくなり、通信効率が向上する。

【００５８】さらに、安全性については、ハッシュ関数は、出力の値から入力の値を得ることは困難であり、また、従来例１のように同じ平文を複数回送信することはないので、十分な安全性が確保できる。加えて、復号誤り検出の後に、再送要求を行い、同じデータを再度送信させるプロトコルを採用する場合においても、平文に乱数が付加されて暗号化されているので、従来例１に示すようなMultiple Transmission Attackに対して、本実施の形態では、従来例１のデータ暗号化システムよりも耐性を持っている。

【００５９】また、従来技術によると、平文をそのまま暗号化して送信しているので、受信者からの再送要求に応じて、送信者が同じ平文を暗号化して生成した暗号文を再送する場合、通信路を傍受する第三者に平文を解読される可能性が高くなる。つまり、第三者が傍受した複数の暗号文から平文が解読される恐れがある。この攻撃方法は、Ｍｕｌｔｉｐｌｅ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ａｔｔａｃｋと呼ばれる。

【００６０】これに対し、本実施の形態によると、通信毎に付加情報Ｒａを異なる内容に設定できるので、受信者からの再送要求に応じて、送信者が暗号文を再送する場合に、平文自体は同じであっても、ｍ｜｜Ｒａの値は、通信の都度異なり、第三者は、Ｍｕｌｔｉｐｌｅ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ａｔｔａｃｋを適用できず、平文が不正に解読される可能性が低くなる。

【００６１】また、通信路の伝送品質が低いために、伝送される暗号文にビット落ちや、ビット化けが発生した場合であっても、上記と同様にして、元の平文と復号文との違いが検出できる。

２．変形例

暗号通信システム１の変形例について、説明する。

【００６２】２．１　付加情報の変形例

暗号通信システム１において、付加情報生成部１０２は、乱数である付加情報Ｒａを生成するとしているが、タイムスタンプ情報又はカウンタ情報を生成するとしてもよい。付加情報生成部１０２が生成する付加情報は、用いる度に異なる値となるものであれば、どのような情報であってもよい。

【００６３】タイムスタンプ情報は、付加情報生成部１０２が付加情報を生成する現在時刻であり、具体的には、年、月、日、時、分、秒、ミリ秒から構成される固定長の情報である。また、カウンタ情報は、固定桁数の数値情報であり、利用される都度、１の値が加算される情報である。

【００６４】２．２　結合情報Ｆ（ｍ、Ｒａ）算出の変形例

暗号通信システム１において、情報付加部１０３は、平文ｍと付加情報Ｒａとを結合して、結合情報Ｆ（ｍ、Ｒａ）＝ｍ｜｜Ｒａを算出するとしているが、算出方法は、付加情報に基づくｍの可逆変換であれば、その他の方法であってもよい。

【００６５】前記算出方法を含めて、その他の算出方法を以下に示す。情報除去部２０３において、結合情報か

ら付加情報を除去して、平文のみを抽出するためには、算出方法に対して、それぞれ逆の演算を行う。

（１）算出方法１

結合情報Ｆ（ｍ、Ｒａ）＝ｍ｜｜Ｒａ

ここで、「｜｜」は、ビット結合を示す。（この算出方法は、上記の実施の形態において示す算出方法である。）

なお、結合情報Ｆ（ｍ、Ｒａ）＝Ｒａ｜｜ｍとしてもよい。

【００６６】また、平文ｍを４ビットずつの複数個の部分平文情報に分割する。また、付加情報を４ビットずつの複数個の部分付加情報に分割する。次に、部分平文情報と部分付加情報とを交互に結合することにより、結合情報を得るとしてもよい。一般に、平文ｍの長さ＞付加情報の長さであるので、結合情報の後部は、部分平文情報のみが結合される。

【００６７】（２）算出方法２

結合情報Ｆ（ｍ、Ｒａ）＝ｍ（＋）Ｒａ

ここで、「（＋）」は、排他的論理和を示す。また、逆の演算は、次の通りである。

復号文ｍ’＝結合情報Ｆ（＋）Ｒａ

（３）算出方法３

結合情報Ｆ（ｍ、Ｒａ）＝ｍ＋Ｒａ

また、逆の演算は、次の通りである。

【００６８】復号文ｍ’＝結合情報Ｆ－Ｒａ

（４）算出方法４

結合情報Ｆ（ｍ、Ｒａ）＝ｍ×Ｒａ　ｍｏｄ　ｐ

ここで、ｐは、ｍより大きい素数である。また、逆の演算は、次の通りである。

【００６９】

復号文ｍ’＝結合情報Ｆ／Ｒａ　ｍｏｄ　ｐ

（５）算出方法５

結合情報Ｆ（ｍ、Ｒａ）＝BitPerm［Ｒａ］（ｍ）

ここで、BitPerm［Ｒａ］（ｍ）は、Ｒａに基づいて、ｍのビット表現を置換する演算を示す。

【００７０】具体的には、以下のような演算である。

（５－１）算出方法５－１

ｍを、Ｒａビットだけ、ビットローテートさせる。

（例）置換前のｍ＝「１１１１０００００１１１１０００００」をとし、Ｒａ＝３（１０進数表現）とすると、置換後のｍ＝「１００００１１１１００００１１１」となる。

【００７１】ここで、逆方向のビットローテートとしてもよい。また、逆の演算は、次の通りである。結合情報Ｆを、Ｒａビットだけ、逆方向へビットローテートさせる。

（５－２）算出方法５－２

ｍを、計算アルゴリズムにより置換する。言い換えると、Ｒａを入力値とする演算をし、その演算結果に基づいて、ｍを、置換する。

【００７２】（例）Ｒａを１２８ビット長とする。Ｒａにハッシュ関数を施して、１６ビット長のハッシュ値を得る。次に、算出方法５－１に示すように、得られたハッシュ値だけ、ｍをビットローテートさせる。また、逆の演算は、次の通りである。結合情報Ｆを、計算アルゴリズムにより置換する。言い換えると、Ｒａを入力値とする演算をし、その演算結果に基づいて、結合情報Ｆを、置換して、復号文ｍ’を得る。

【００７３】（例）Ｒａを１２８ビット長とする。Ｒａにハッシュ関数を施して、１６ビット長のハッシュ値を得る。次に、算出方法５－１に示すように、得られたハッシュ値だけ、結合情報Ｆを逆方向にビットローテートさせる。

（５－３）算出方法５－３

ｍを４ビットずつに区切って複数の部分情報を生成する。次に、部分情報毎に、Ｒａに対応する入出力４ビットの置換テーブルを用いて、置換する。

【００７４】ここで、置換テーブルは、４ビットの変換前ビット列と対応する４ビットの変換後ビット列とからなる組を、１６個含む。ある値（例えば、「１」）のＲａに対応する置換テーブルにおいて、１６個の変換前ビット列は、「００００」、「０００１」、「００１０」、・・・、「１１１０」及び「１１１１」である。これらに対応する１６個の変換後ビット列は、「１１１１」、「１１１０」、「１１０１」、・・・、「０００１」及び「００００」である。

【００７５】また、別の値（例えば、「２」）のＲａに対応する置換テーブルにおいて、１６個の変換前ビット列に対応する１６個の変換後ビット列は、「１１１１」、「１１１０」、「１１０１」、・・・、「００００」及び「０００１」である。このように、Ｒａの値に対応して複数種類の置換テーブルが存在する。また、逆の演算は、次の通りである。

【００７６】結合情報Ｆを４ビットずつに区切って複数の部分結合情報を生成する。次に、部分結合情報毎に、Ｒａに対応する入出力４ビットの置換テーブルを用いて、上記の逆方向の置換を行う。

（６）算出方法６

結合情報Ｆ（ｍ、Ｒａ）＝Ｔａｂ［Ｒａ］（ｍ）

ここで、Ｔａｂ［Ｒａ］（ｍ）は、ｍを変換テーブルＴａｂに従って変換することを示す。

【００７７】例えば、ｍが８ビット長の場合、Ｒａの値毎に、例えば、図７に示すような変換テーブルＴａｂを記憶しておき、変換テーブルＴａｂに従って、ｍの値を変換する。変換テーブルＴａｂは、８ビットの値と８ビットの値を対応付けた組を２５６個含む。例えば、ｍ＝１の場合、図７に示す変換テーブルＴａｂに基づいて、平文ｍは、３９に変換される。

【００７８】また、逆の演算は、次の通りである。結合情報Ｆを変換テーブルＴａｂに従って、上記と逆方向に

変換する。

２．３　付加情報を共有するための暗号通信システムの変形例

送信装置１０と受信装置２０とにおいて、付加情報を共有するための暗号通信システムの変形例について、以下に説明する。

【００７９】（１）第１の変形例

暗号通信システム１の第１の変形例としての暗号通信システム１ｂについて説明する。

（暗号通信システム１ｂの構成）暗号通信システム１ｂは、図８に示すように、送信装置１０ｂ及び受信装置２０ｂから構成される。

【００８０】送信装置１０ｂ及び受信装置２０ｂは、それぞれ、暗号通信システム１を構成する送信装置１０及び受信装置２０と、同様の構成を有している。以下において、送信装置１０及び受信装置２０との相違点を中心として説明する。送信装置１０ｂは、さらに、同期部１０７を備えている。また、送信装置１０ｂは、付加情報生成部１０２に代えて、付加情報生成部１０２ｂを備えている。また、受信装置２０ｂは、さらに、同期部２０８及び付加情報生成部２０９を備えている。同期部１０７と同期部２０８とは、専用回線４０ｂを介して接続されている。

【００８１】同期部１０７は、乱数ＸＲを生成し、生成した乱数ＸＲを専用回線４０ｂを介して同期部２０８へ出力する。また、生成した乱数ＸＲを付加情報生成部１０２へ出力する。付加情報生成部１０２は、同期部１０７から乱数ＸＲを受け取り、受け取った乱数ＸＲを用いて、付加情報Ｒａを生成し、生成した付加情報Ｒａを情報付加部１０３へ出力する。ここで、乱数ＸＲを用いて付加情報Ｒａを生成する一例として、付加情報生成部１０２は、乱数ＸＲをそのまま付加情報Ｒａとする。

【００８２】同期部２０８は、専用回線４０ｂを介して、付加情報ＸＲを受け取り、受け取った付加情報ＸＲを付加情報生成部２０９へ出力する。付加情報生成部２０９は、同期部２０８から乱数ＸＲを受け取り、受け取った乱数ＸＲを用いて、付加情報Ｒａを生成し、生成した付加情報Ｒａを情報除去部２０３へ出力する。ここで、乱数ＸＲを用いて付加情報Ｒａを生成する一例として、付加情報生成部２０９は、乱数ＸＲをそのまま付加情報Ｒａとする。

【００８３】（暗号通信システム１ｂの動作）暗号通信システム１ｂの動作について、図９に示すフローチャートを用いて説明する。なお、暗号通信システム１ｂの動作は、暗号通信システム１の動作と同様であるので、ここでは相違点を中心として説明する。

【００８４】同期部１０７は、乱数ＸＲを生成し（ステップＳ２０１）、生成した乱数ＸＲを専用回線４０ｂを介して同期部２０８へ出力する（ステップＳ２０２）。また、生成した乱数ＸＲを付加情報生成部１０２へ出力する（ステップＳ２０３）。付加情報生成部１０２は、同期部１０７から乱数ＸＲを受け取り、受け取った乱数ＸＲを用いて、付加情報Ｒａを生成し、生成した付加情報Ｒａを情報付加部１０３へ出力する（ステップＳ２０３）。

【００８５】同期部２０８は、専用回線４０ｂを介して、乱数ＸＲを受け取り、受け取った乱数ＸＲを付加情報生成部２０９へ出力する（ステップＳ２０２）。付加情報生成部２０９は、同期部２０８から乱数ＸＲを受け取り、受け取った乱数ＸＲを用いて、付加情報Ｒａを生成し（ステップＳ２０４）、生成した付加情報Ｒａを情報除去部２０３へ出力する（ステップＳ２０５）。情報除去部２０３は、付加情報Ｒａを受け取り（ステップＳ２０５）、受け取った付加情報Ｒａを用いて、復号結合情報から復号文ｍ’を生成する（ステップＳ２０６）。

【００８６】（２）第２の変形例

暗号通信システム１の第２の変形例としての暗号通信システム１ｃについて説明する。

（暗号通信システム１ｃの構成）暗号通信システム１ｃは、図１０に示すように、送信装置１０ｃ及び受信装置２０ｃから構成される。

【００８７】送信装置１０ｃ及び受信装置２０ｃは、それぞれ、暗号通信システム１を構成する送信装置１０及び受信装置２０と、同様の構成を有している。送信装置１０ｃは、付加情報生成部１０２及び送信部１０６に代えて、付加情報生成部１０２ｃ及び送信部１０６ｃを備えている。また、受信装置２０ｃは、情報除去部２０３及び受信部２０１に代えて、情報除去部２０３ｃ及び受信部２０１ｃを備えている。

【００８８】付加情報生成部１０２ｃ、送信部１０６ｃ、情報除去部２０３ｃ及び受信部２０１ｃは、それぞれ付加情報生成部１０２、送信部１０６、情報除去部２０３及び受信部２０１と同様の構成を有している。以下において相違点を中心として説明する。付加情報生成部１０２ｃは、生成した付加情報Ｒａを送信部１０６ｃへ出力する。

【００８９】送信部１０６ｃは、付加情報生成部１０２ｃから付加情報Ｒａを受け取り、受け取った付加情報Ｒａをインターネット３０を介して、受信装置２０ｃへ送信する。受信部２０１ｃは、送信装置１０ｃからインターネット３０を介して、付加情報Ｒａを受信し、受信した付加情報Ｒａを情報除去部２０３ｃへ出力する。

【００９０】情報除去部２０３ｃは、受信部２０１から付加情報Ｒａを受け取り、受け取った付加情報Ｒａを用いて、復号結合情報から復号文ｍ’を生成する。

（暗号通信システム１ｃの動作）暗号通信システム１ｃの動作について、図１１に示すフローチャートを用いて説明する。

【００９１】なお、暗号通信システム１ｃの動作は、暗号通信システム１の動作と同様であるので、ここでは相

違点を中心として説明する。付加情報生成部１０２ｃは、付加情報Ｒａを生成し、生成した付加情報Ｒａを送信部１０６ｃへ出力する（ステップＳ２２１）。送信部１０６ｃは、付加情報生成部１０２ｃから付加情報Ｒａを受け取り、受け取った付加情報Ｒａをインターネット３０を介して、受信装置２０ｃへ送信する（ステップＳ２２２）。

【００９２】受信部２０１ｃは、送信装置１０ｃからインターネット３０を介して、付加情報Ｒａを受信し、受信した付加情報Ｒａを情報除去部２０３ｃへ出力する（ステップＳ２２２）。情報除去部２０３ｃは、受信部２０１から付加情報Ｒａを受け取り（ステップＳ２２３）、受け取った付加情報Ｒａを用いて、復号結合情報から復号文m'を生成する（ステップＳ２２４）。

【００９３】（３）第３の変形例

暗号通信システム１の第３の変形例としての暗号通信システム１ｄについて説明する。

（暗号通信システム１ｄの構成）暗号通信システム１ｄは、図１２に示すように、送信装置１０ｄ及び受信装置２０ｄから構成される。

【００９４】送信装置１０ｄ及び受信装置２０ｄは、それぞれ、暗号通信システム１を構成する送信装置１０及び受信装置２０と、同様の構成を有している。送信装置１０ｄは、付加情報生成部１０２、暗号化部１０５及び送信部１０６に代えて、付加情報生成部１０２ｄ、暗号化部１０５ｄ及び送信部１０６ｄを備えている。また、受信装置２０ｄは、復号化部２０２、情報除去部２０３及び受信部２０１に代えて、復号化部２０２ｄ、情報除去部２０３ｄ及び受信部２０１ｄを備えている。

【００９５】付加情報生成部１０２ｄ、暗号化部１０５ｄ、送信部１０６ｄ、復号化部２０２ｄ、情報除去部２０３ｄ及び受信部２０１ｄは、それぞれ付加情報生成部１０２、暗号化部１０５、送信部１０６、復号化部２０２、情報除去部２０３及び受信部２０１と同様の構成を有している。以下において相違点を中心として説明する。

【００９６】付加情報生成部１０２ｄは、付加情報Ｒａを生成し、生成した付加情報Ｒａを暗号化部１０５ｄへ出力する。暗号化部１０５ｄは、付加情報生成部１０２ｄから付加情報Ｒａを受け取り、受け取った付加情報Ｒａに暗号アルゴリズムを施して、暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を生成する。ここで、ｒ２は、ｒと同様の乱数である。次に、生成した暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を送信部１０６ｄへ出力する。

【００９７】送信部１０６ｄは、暗号化部１０５ｄから暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を受け取り、受け取った暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）をインターネット３０を介して、受信装置２０ｄへ送信する。受信部２０１ｄは、受信装置２０ｄからインターネット３０を介して、暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）

を受信し、受信した暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を復号化部２０２ｄへ出力する。

【００９８】復号化部２０２ｄは、受信部２０１ｄから暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を受け取り、受け取った暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）に復号アルゴリズムを施して、復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を生成する。次に、生成した復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を情報除去部２０３ｄへ出力する。

【００９９】情報除去部２０３ｄは、復号化部２０２ｄから復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を受け取り、受け取った復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を用いて、復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ）から復号文m'を生成する。

（暗号通信システム１ｄの動作）暗号通信システム１ｄの動作について、図１３に示すフローチャートを用いて説明する。

【０１００】なお、暗号通信システム１ｄの動作は、暗号通信システム１の動作と同様であるので、ここでは相違点を中心として説明する。付加情報生成部１０２ｄは、付加情報Ｒａを生成し、生成した付加情報Ｒａを暗号化部１０５ｄへ出力する（ステップＳ２４１）。暗号化部１０５ｄは、付加情報生成部１０２ｄから付加情報Ｒａを受け取り、受け取った付加情報Ｒａに暗号アルゴリズムを施して、暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を生成し、生成した暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を送信部１０６ｄへ出力する（ステップＳ２４２）。

【０１０１】送信部１０６ｄは、暗号化部１０５ｄから暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を受け取り、受け取った暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）をインターネット３０を介して、受信装置２０ｄへ送信する（ステップＳ２４３）。受信部２０１ｄは、受信装置２０ｄからインターネット３０を介して、暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を受信し、受信した暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を復号化部２０２ｄへ出力する（ステップＳ２４３）。

【０１０２】復号化部２０２ｄは、受信部２０１ｄから暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）を受け取り、受け取った暗号化付加情報Ｅ（Ｒａ、Ｋｐ、ｒ２）に復号アルゴリズムを施して、復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を生成し、生成した復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を情報除去部２０３ｄへ出力する（ステップＳ２４４）。

【０１０３】情報除去部２０３ｄは、復号化部２０２ｄから復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を受け取り（ステップＳ２４５）、受け取った復号付加情報Ｄ（Ｅ（Ｒａ、Ｋｐ、ｒ２）、Ｋｓ）を用いて、復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋ

ｓ）から復号文ｍ’を生成する（ステップＳ２４６）。

２．４　変形例の実現可能な組合せ

付加情報の変形例、結合情報Ｆ（ｍ、Ｒａ）算出の変形例、及び付加情報を共有するための暗号通信システム変形例の、実現可能な組合せについて、図１４に示す表を用いて説明する。

【０１０４】この表に示すように、付加情報の各変形例（乱数、タイムスタンプ及びカウンタ）は、結合情報Ｆ（ｍ、Ｒａ）算出の変形例、及び付加情報を共有するための暗号通信システム変形例において、適用可能である。また、この表に示すように、結合情報Ｆ（ｍ、Ｒａ）算出の変形例のうち、ｍ｜｜Ｒａによる結合情報の算出方法は、暗号通信システム１、１ｂ～１ｄにおいて、適用可能である。

【０１０５】また、この表に示すように、結合情報Ｆ（ｍ、Ｒａ）算出の変形例のうち、ｍ（＋）Ｒａ、ｍ＋Ｒａ、ｍ×Ｒａ　ｍｏｄ　ｐ、ＢｉｔＰｅｒｍ［Ｒａ］（ｍ）、Ｔａｂ［Ｒａ］（ｍ）による結合情報の算出方法は、暗号通信システム１ｂ～１ｄにおいて、適用可能である。

３．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

【０１０６】（１）暗号通信システム１は、次のように構成してもよい。

送信装置１０の一方向性関数部１０４は、情報付加部１０３から結合情報Ｆ（ｍ、Ｒａ）を受け取り、受け取った結合情報Ｆ（ｍ、Ｒａ）にハッシュ関数を施して、関数値ｈ（Ｆ（ｍ、Ｒａ））を生成し、生成した関数値ｈ（Ｆ（ｍ、Ｒａ））を送信部１０６、インターネット３０、受信部２０１を介して、比較部２０５へ送信する。

【０１０７】一方、受信装置２０の一方向性関数部２０４は、復号化部２０２から復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ）を受け取り、受け取った復号結合情報Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ）にハッシュ関数を施して、関数値ｈ（Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ））を生成し、生成した関数値ｈ（Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ））を比較部２０５へ出力する。比較部２０５は、関数値ｈ（Ｆ（ｍ、Ｒａ））と、関数値ｈ（Ｄ（Ｅ（Ｆ（ｍ、Ｒａ）、Ｋｐ、ｒ）、Ｋｓ））を比較して、一致するか否かを判断する。

【０１０８】このようにして、平文が正しく復号できたか否かを判断することができる。

（２）暗号通信システム１は、次のように構成してもよい。

送信装置１０の情報付加部１０３は、さらに、Ｆとは異なる可逆変換であるＧを用いて、結合情報Ｇ（ｍ、Ｒａ）を生成する。ここで、Ｇの具体例は、Ｇ＝Ｒａ｜｜ｍである。次に、情報付加部１０３は、生成した結合情報Ｇ（ｍ、Ｒａ）を一方向性関数部１０４へ出力する。一方向性関数部１０４は、情報付加部１０３から結合情報Ｇ（ｍ、Ｒａ）を受け取り、受け取った結合情報Ｇ（ｍ、Ｒａ）にハッシュ関数を施して、関数値ｈ（Ｇ（ｍ、Ｒａ））を生成し、生成した関数値ｈ（Ｇ（ｍ、Ｒａ））を送信部１０６、インターネット３０、受信部２０１を介して、比較部２０５へ送信する。

【０１０９】一方、受信装置２０の情報除去部２０３は、さらに、生成した復号文ｍ’及び乱数ＲａにＧを用いて、結合情報Ｇ（ｍ’、Ｒａ）を生成して、一方向性関数部２０４へ出力する。ここで、情報除去部２０３は、上述の変形例に示すようにして、送信装置１０との間で同じ乱数Ｒａを共有する。一方向性関数部２０４は、結合情報Ｇ（ｍ’、Ｒａ）を受け取り、受け取った結合情報Ｇ（ｍ’、Ｒａ）にハッシュ関数を施して、関数値ｈ（Ｇ（ｍ’、Ｒａ））を生成し、生成した関数値ｈ（Ｇ（ｍ’、Ｒａ））を比較部２０５へ出力する。比較部２０５は、関数値ｈ（Ｇ（ｍ、Ｒａ））と関数値ｈ（Ｇ（ｍ’、Ｒａ））とを比較して、一致するか否かを判断する。

【０１１０】このようにして、平文が正しく復号できたか否かを判断することができる。

（３）暗号アルゴリズム及び復号アルゴリズムは、上記の実施の形態に示したアルゴリズムに限定されない。他の暗号アルゴリズムを適用してもよい。例えば、ＤＥＳ暗号方式、ＲＳＡ暗号方式やＥＩＧａｍａＩ暗号方式などの一般の暗号方式が適用できる。

【０１１１】また、一方向性関数部１０４は、ハッシュ関数以外に、前記一般の暗号方式の暗号化関数などの一方向性関数を用いてもよい。なお、ＤＥＳ暗号方式、ＲＳＡ暗号方式、及びＥＩＧａｍａＩ暗号方式については、岡本龍明、山本博資、“現代暗号”、シリーズ／情報科学の数学、産業図書、１９９７に詳しく述べられている。

【０１１２】さらに、システム利用者全体で一方向性関数を共有せずに、送信側及び受信側のユーザ組毎に一方向性関数が異なっていてもよい。

（４）本実施の形態では、送信装置１０と受信装置２０とは、インターネット３０を介して接続されているとしているが、インターネットには限定されない。専用回線、無線通信路などにより接続されているとしてもよい。

【０１１３】（５）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み

取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、ＣＤ—ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１１４】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０１１５】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（６）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１１６】

【発明の効果】上記目的を達成するために、本発明は、平文を暗号化して暗号文を得、前記平文に一方向性関数を施して第１関数値を得、前記暗号文と前記第１関数値とを送信する送信装置、及び前記暗号文と前記第１関数値とを受信し、前記暗号文を復号して復号文を得、前記復号文に前記一方向性関数を施して第２関数値を得、前記第２関数値と前記第１関数値とが一致する場合に、前記復号文は前記平文に一致すると判断する受信装置から構成される暗号通信システムであって、送信装置は、第１付加情報を生成する第１生成手段と、前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成する可逆演算手段と、前記結合情報に暗号アルゴリズムを施して暗号文を生成する暗号手段と、前記暗号文を送信する送信手段とを含み、受信装置は、前記暗号文を受信する受信手段と、前記第１付加情報と同一の第２付加情報を生成する第２生成手段と、前記暗号文に、前記暗号アルゴリズムの逆変換である復号アルゴリズムを施して復号結合情報を生成する復号手段と、前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成する逆可逆演算手段とを含む。

【０１１７】この構成によると、前記送信装置は、前記平文及び前記第１付加情報に可逆演算を施して、結合情報を生成し、前記結合情報を暗号化して暗号化結合情報を生成して送信し、前記受信装置は、前記暗号化結合情報を受信して復号して復号結合情報を生成し、前記復号結合情報及び第２付加情報に前記可逆演算の逆演算を施して、復号文を生成するので、従来技術よりもさらに安全性の高い暗号通信システムを実現できる。

【０１１８】ここで、前記第１生成手段及び前記第２生成手段は、同期して、それぞれ同一内容の第１付加情報及び第２付加情報を生成する。この構成によると、前記第１生成手段及び前記第２生成手段が、同期して、それぞれ同一内容の第１付加情報及び第２付加情報を生成するので、結合情報と同一内容の復号結合情報が得られると期待できる。

【０１１９】ここで、前記第１生成手段は、乱数を生成し、生成した乱数を前記第１付加情報とする。この構成によると、前記第１生成手段は、乱数を用いて第１付加情報を生成するので、通信毎に第１付加情報が異なり、暗号化結合情報から第１付加情報を推定することが困難となる。

【０１２０】ここで、前記可逆演算手段は、前記平文及び前記第１付加情報に、ビット結合を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第２付加情報を削除して復号文を生成する。この構成によると、前記可逆演算手段は、前記平文及び前記第１付加情報に、ビット結合を施して、結合情報を生成し、前記逆可逆演算手段は、前記復号結合情報から前記第２付加情報を削除して復号文を生成するので、前記復号結合情報から確実に復号文を生成することができる。

【図面の簡単な説明】

【図１】暗号通信システム１の構成を示すブロック図である。

【図２】暗号化部１０５の構成を示すブロック図である。

【図３】復号化部２０２の構成を示すブロック図である。

【図４】送信装置１０の動作を示すフローチャートである。図５に続く。

【図５】送信装置１０の動作を示すフローチャートである。図４から続く。

【図６】受信装置２０の動作を示すフローチャートである。

【図７】算出方法６において用いられる変換テーブルの一例を示す。

【図８】暗号通信システム１の第１の変形例としての暗号通信システム１ｂの構成を示すブロック図である。

【図９】暗号通信システム１ｂの動作を示すフローチャートである。

【図１０】暗号通信システム１の第２の変形例としての暗号通信システム１ｃの構成を示すブロック図である。

【図１１】暗号通信システム１ｃの動作を示すフローチャートである。

【図１２】暗号通信システム１の第３の変形例としての暗号通信システム１ｄの構成を示すブロック図である。

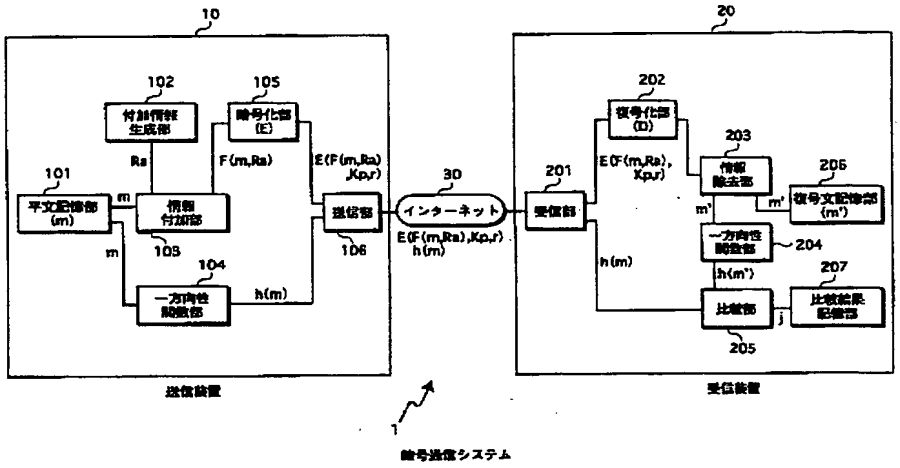
【図１３】暗号通信システム１ｄの動作の動作を示すフローチャートである。

【図１４】変形例の実現可能な組合せを示す表である。

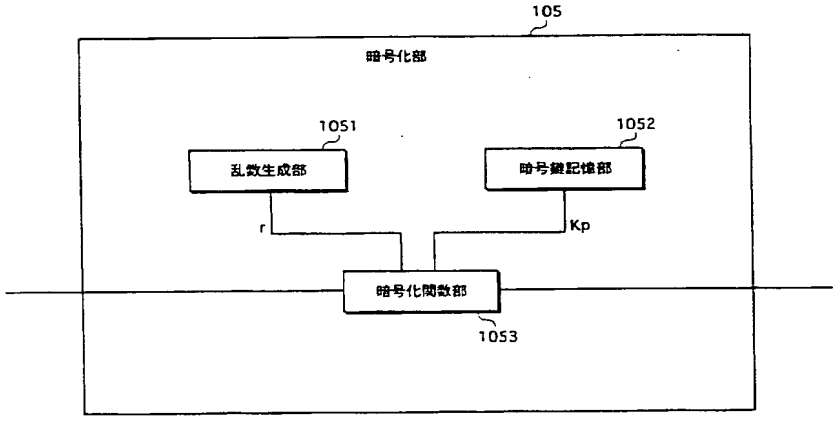
【符号の説明】

１　暗号通信システム
１０　送信装置
２０　受信装置
３０　インターネット
１０１　平文記憶部
１０２　付加情報生成部
１０３　情報付加部
１０４　一方向性関数部
１０５　暗号化部
１０６　送信部
２０１　受信部
２０２　復号化部
２０３　情報除去部
２０４　一方向性関数部
２０５　比較部
２０６　復号文記憶部
２０７　比較結果記憶部
２０９　付加情報生成部

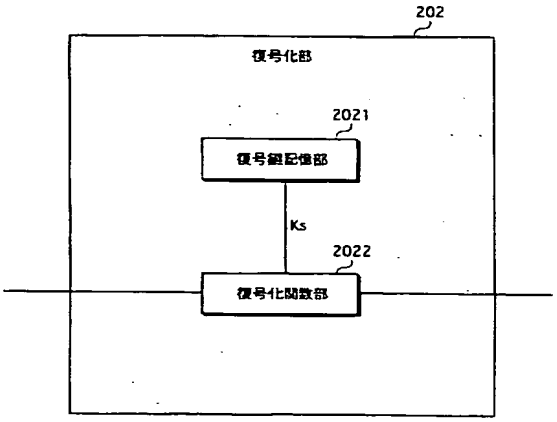
【図１】



【図２】



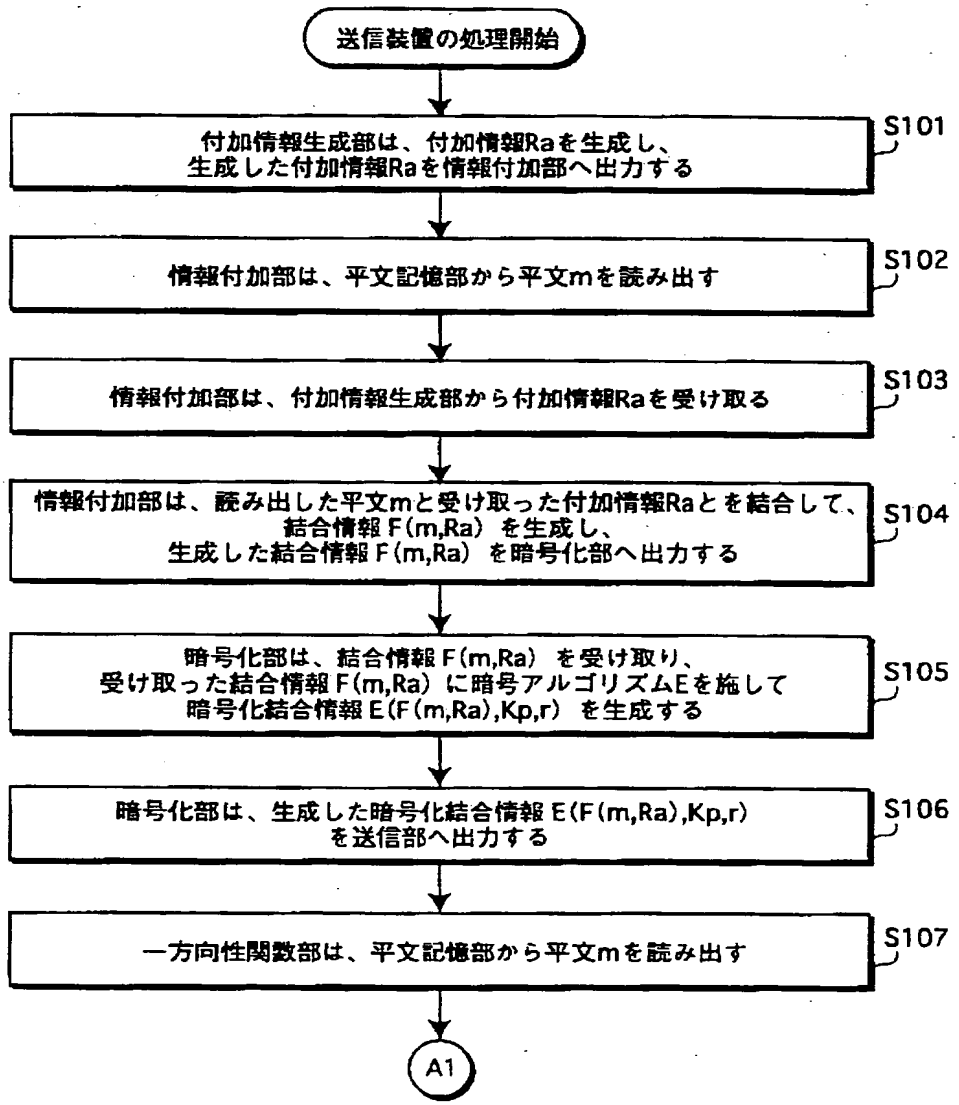
【図３】



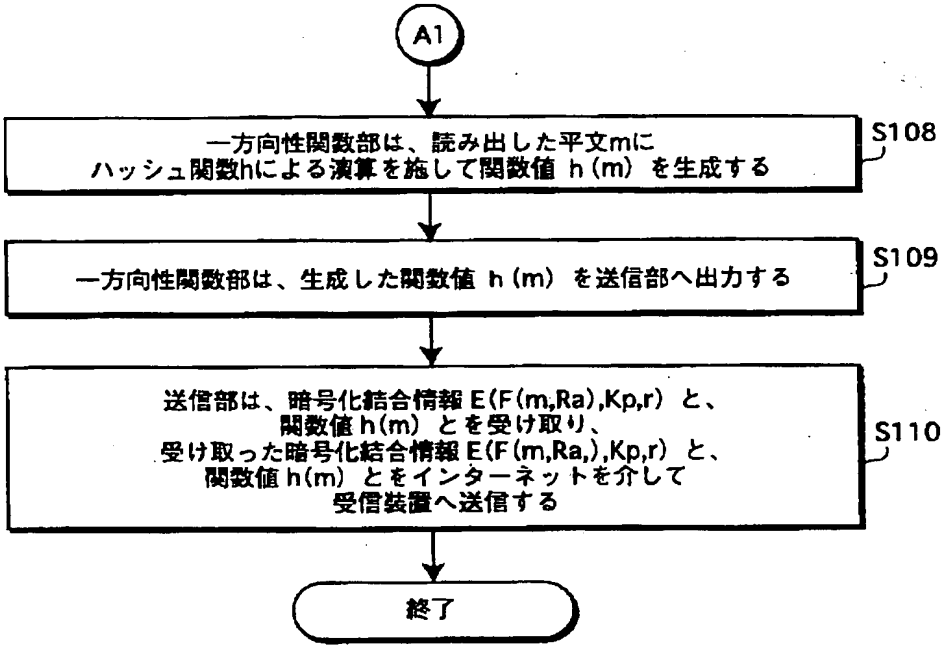
【図１４】

付加情報 / 可逆変換 F(m,Ra)	(1) Ra: 乱数	(2) Ra: タイムスタンプ	(3) Ra: カウンタ
(1) m∥Ra	暗号通信システム 1,1b~1d		
(2) m⊕Ra	暗号通信システム 1b~1d		
(3) m+Ra			
(4) m×Ra mod p			
(5) BitPerm[Ra](m)			
(6) Tab[Ra](m)			

【図４】



【図５】

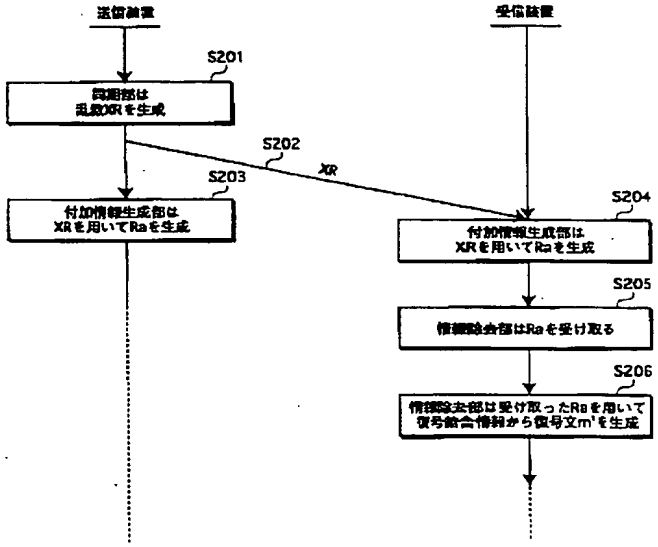


【図７】

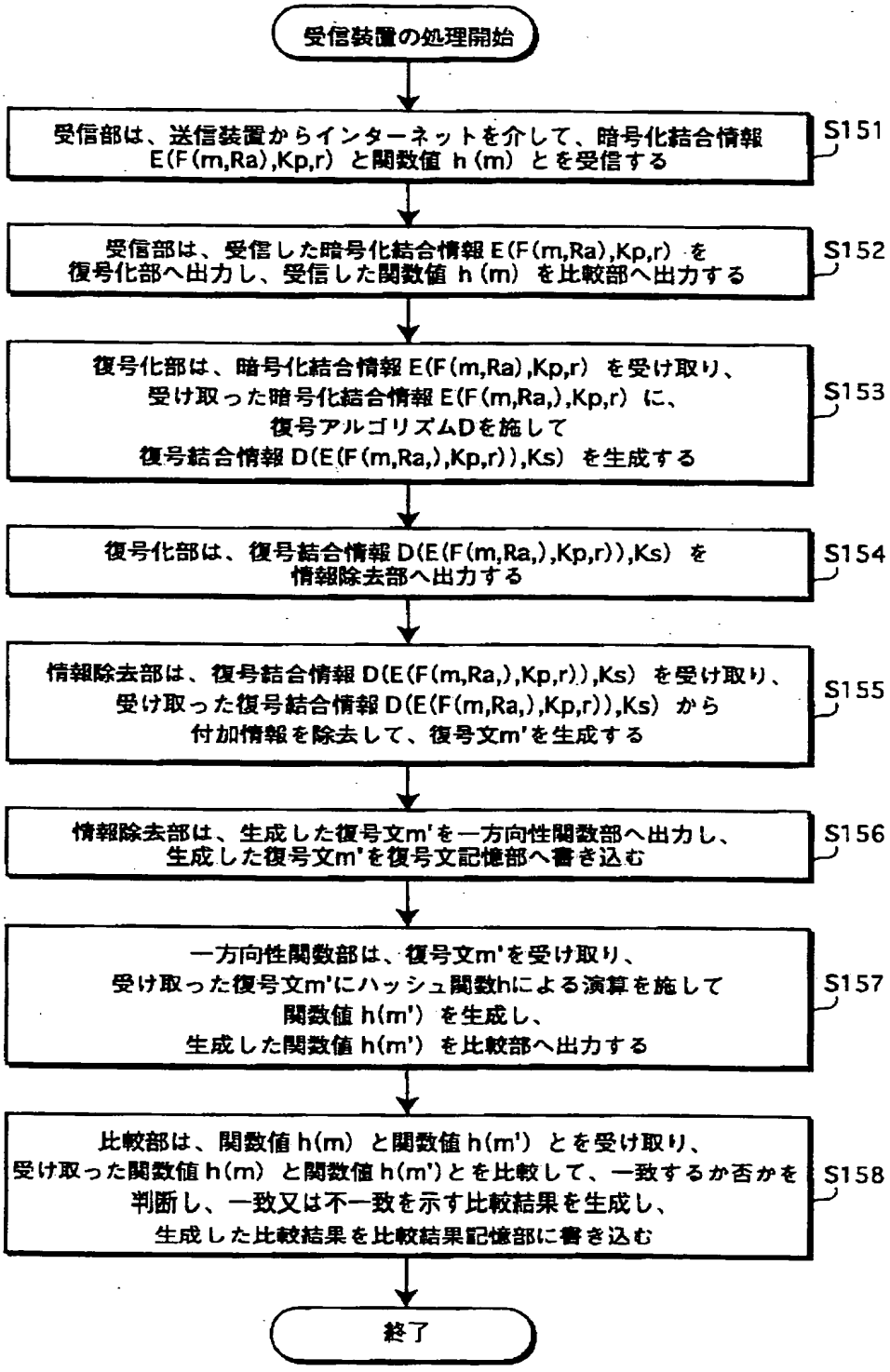
変換テーブル

入力値m	出力値 Tab[Ra](m)
0	122
1	39
・ ・ ・ ・ ・	・ ・ ・ ・ ・
255	91

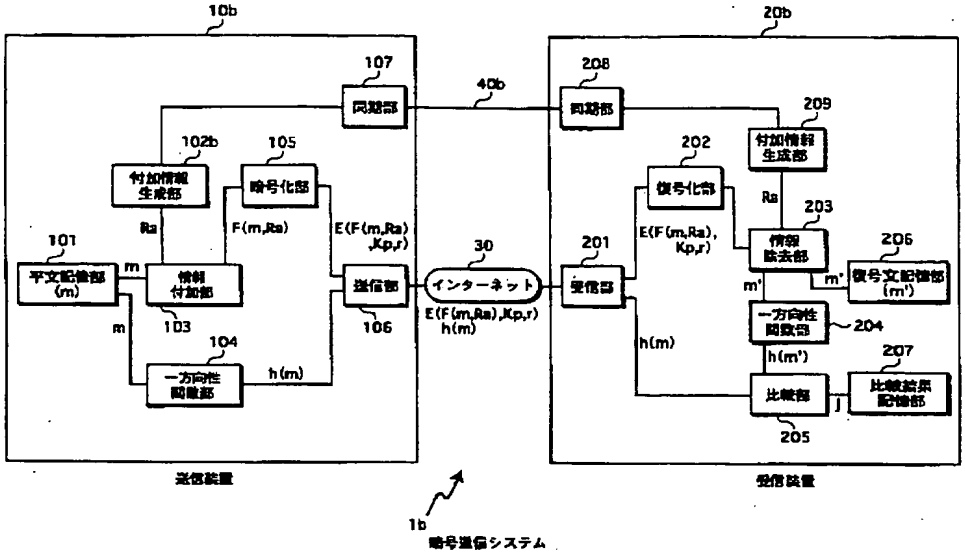
【図９】



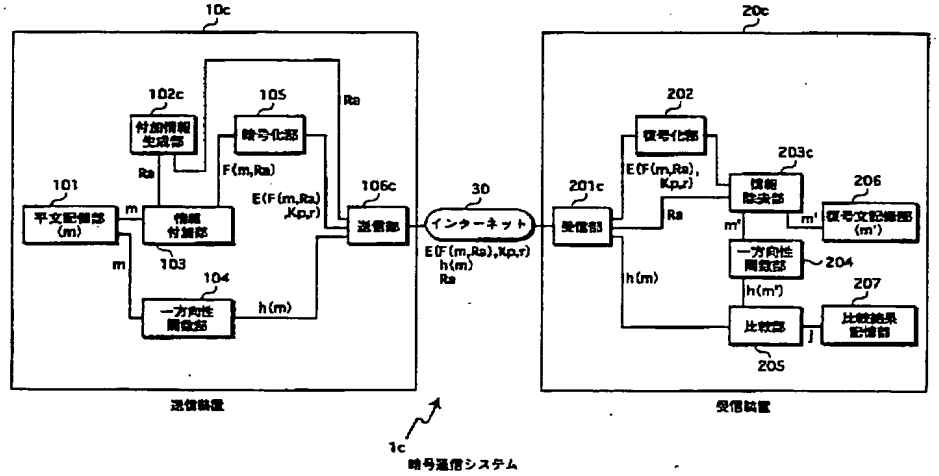
【図６】


受信装置の処理開始
受信部は、送信装置からインターネットを介して、暗号化結合情報E(F(m,Ra),Kp,r) と関数値 h(m) とを受信する
S151
受信部は、受信した暗号化結合情報 E(F(m,Ra),Kp,r) を復号化部へ出力し、受信した関数値 h(m) を比較部へ出力する
S152
復号化部は、暗号化結合情報 E(F(m,Ra),Kp,r) を受け取り、受け取った暗号化結合情報 E(F(m,Ra,),Kp,r) に、復号アルゴリズムDを施して復号結合情報 D(E(F(m,Ra,),Kp,r)),Ks) を生成する
S153
復号化部は、復号結合情報 D(E(F(m,Ra,),Kp,r)),Ks) を情報除去部へ出力する
S154
情報除去部は、復号結合情報 D(E(F(m,Ra,),Kp,r)),Ks) を受け取り、受け取った復号結合情報 D(E(F(m,Ra,),Kp,r)),Ks) から付加情報を除去して、復号文m'を生成する
S155
情報除去部は、生成した復号文m'を一方向性関数部へ出力し、生成した復号文m'を復号文記憶部へ書き込む
S156
一方向性関数部は、復号文m'を受け取り、受け取った復号文m'にハッシュ関数hによる演算を施して関数値 h(m') を生成し、生成した関数値 h(m') を比較部へ出力する
S157
比較部は、関数値 h(m) と関数値 h(m') とを受け取り、受け取った関数値 h(m) と関数値 h(m') とを比較して、一致するか否かを判断し、一致又は不一致を示す比較結果を生成し、生成した比較結果を比較結果記憶部に書き込む
S158
終了

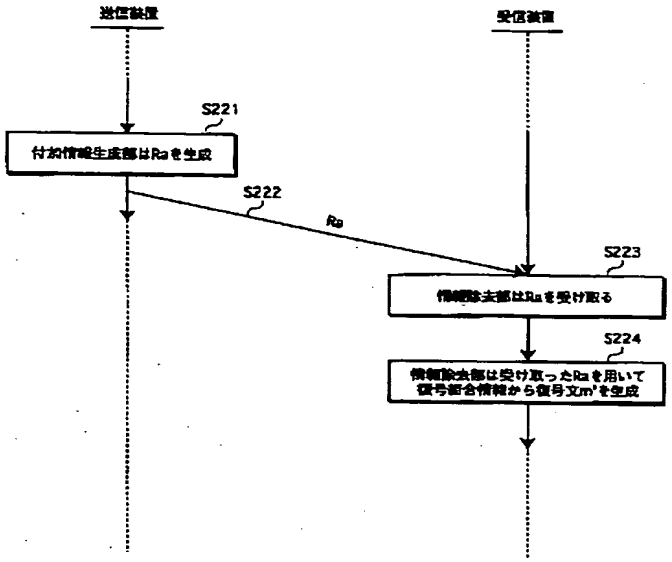
【図８】


10b
20b
107
同期部
40b
208
同期部
209
付加情報生成部
102b
付加情報生成部
105
暗号化部
202
復号化部
Ra
F(m,Ra)
E(F(m,Ra),Kp,r)
E(F(m,Ra),Kp,r)
203
情報除去部
101
平文記憶部(m)
m
情報付加部
30
インターネット
201
受信部
206
復号文記憶部(m')
m'
103
106
E(F(m,Ra),Kp,r)
h(m)
一方向性関数部
204
104
h(m)
h(m')
207
比較結果記憶部
比較部
205
送信装置
受信装置
1b
暗号通信システム

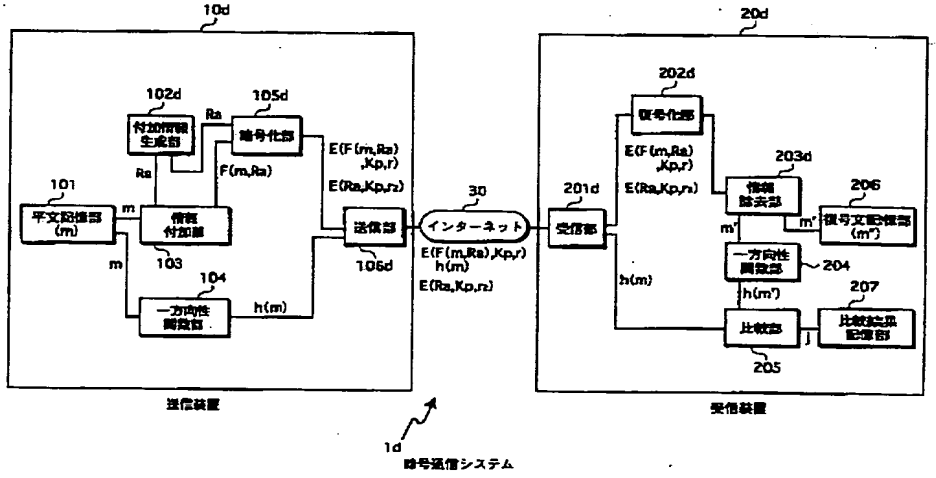
【図１０】


10c
20c
202
102c
105
Ra
復号化部
付加情報生成部
暗号化部
203c
Ra
F(m,Ra)
E(F(m,Ra),Kp,r)
E(F(m,Ra),Kp,r)
情報除去部
206
101
平文記憶部(m)
m
情報付加部
106c
30
インターネット
201c
受信部
復号文記憶部(m')
m'
103
E(F(m,Ra),Kp,r)
h(m)
Ra
一方向性関数部
204
104
h(m)
h(m')
207
比較結果記憶部
比較部
205
送信装置
受信装置
1c
暗号通信システム

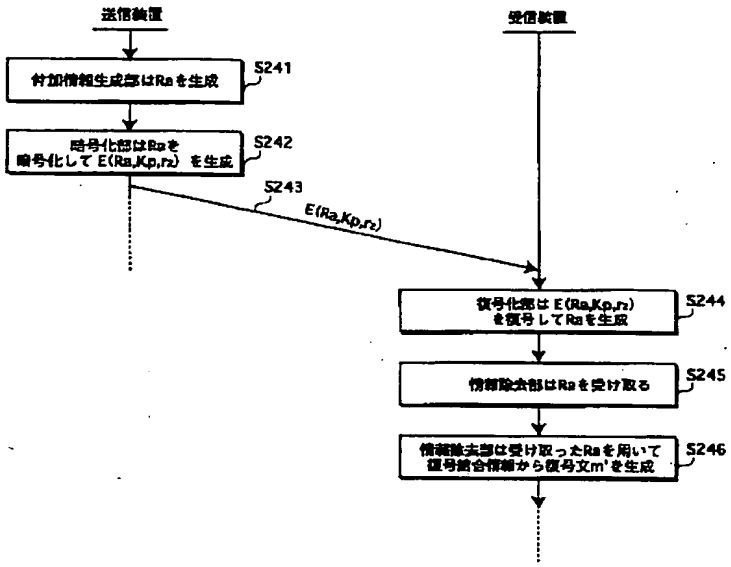
【図１１】


送信装置
受信装置
S221
付加情報生成部はRaを生成
S222
Ra
S223
情報除去部はRaを受け取る
S224
情報除去部は受け取ったRaを用いて
復号結合情報から復号文m'を生成

【図１２】


10d
102d
105d
付加情報生成部
暗号化部
Ra
F(m,Ra)
E(F(m,Ra),Kp,r)
E(Ra,Kp,r2)
101
平文記憶部(m)
m
情報付加部
103
104
一方向性関数部
h(m)
送信部
106d
30
インターネット
E(F(m,Ra),Kp,r)
h(m)
E(Ra,Kp,r2)
送信装置
20d
202d
復号化部
E(F(m,Ra),Kp,r)
E(Ra,Kp,r2)
203d
情報除去部
206
復号文記憶部(m')
m'
一方向性関数部
204
h(m')
207
比較対象記憶部
比較部
205
201d
受信部
h(m)
受信装置
1d
暗号通信システム

【図１３】



フロントページの続き

(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器
産業株式会社内

Ｆターム(参考)　5J104 AA28 FA07 JA04 NA11